AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application:

Listing of Claims:

1. (Previously Presented) A wireless network detection system comprising:

a connection component that can connect a device to a plurality of wireless networks; and,

a detection component that automatically identifies an encryption type of an available wireless network, wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence.

2. (Original) The system of claim 1, identification by the detection component being based, at least in part, upon receipt of an information element from a wireless network beacon.

3. (Original) The system of claim 1, the wireless network comprising at least one of an unencrypted network, a Wired Equivalent Privacy (WEP) network requiring a WEP key, a Wi-Fi Protected Access (WPA) encrypted network requiring a WPA pre-shared key, an 802.1x-enabled network that does not support WPA, an 802.1x-enabled network that does support WPA and a wireless provisioning services (WPS) support-enabled network.

4. (Original) The system of claim 1, identification by the detection component being based, at least in part, upon iterative probing of the available network.

5. (Original) The system of claim 4, wherein the detection component attempts to connect to the wireless network as a wireless provisioning services-supporting network, the detection component determining that the network is a pre-shared key network if a failure in an authentication sequence from a wireless network beacon is determined.

6. (Original) The system of claim 5, the detection component determining that the network is a Wi-Fi Protected Access network if a failure in a particular piece of the authentication sequence that identifies a wireless provisioning services supporting network is determined.

7. (Original) The system of claim 6, the particular piece of the authentication sequence comprising a type, length value sequence.

8. (Original) The system of claim 6, the detection component determining that the network is a wireless provisioning services supporting network if the particular piece of authentication sequence identifying the wireless provisioning services supporting network is received from the wireless network beacon.

9. (Previously Presented) The system of claim 1, wherein the detection component sends at least one of a connect message, an 802.1x Extensible Authentication Protocol Over Lan (EAPOL) start message, an 802.1x identity message.

10. (Original) The system of claim 1, wherein the detection component receives at least one of an associated message, an 802.1x identity request message, an authentication message and a provisioning message from a wireless network beacon.

11. (Cancelled)

12. (Previously Presented) A method facilitating wireless network detection comprising:

attempting to connect to a wireless network as a wireless provisioning services supporting network;

automatically identifying the encryption type of the wireless network, wherein identification of the encryption type is based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence

determining whether the attempt was successful; and,

prompting for a wired equivalent privacy key, if the attempt was not successful.

13. (Previously Presented) The method of claim 12 further comprising at least one of the following acts:

waiting up to a threshold period of time for a particular piece of authentication information that identifies a wireless provisioning services supporting network;

determining whether the particular piece of authentication information has been received;

identifying the wireless network as a Wi-Fi Protected Access (WAP) network, if the particular piece of authentication information has not been received; and,

identifying the wireless network as a wireless provisioning services supporting network, if the particular piece of authentication information has been received.

14. (Cancelled)

15. (Currently Amended) A method facilitating wireless network detection comprising:

determining whether a wireless network supports 802.1x, based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence;

identifying the wireless network as an wired equivalent privacy network requiring a wired equivalent privacy key, if the wireless network does not support 802.1x.

determining whether the wireless network supports wireless provisioning services[[,]] if the wireless network supports 802.1x based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence; and,

identifying the wireless network as an 802.1x network, if the wireless network does not supporting wireless provisioning services; and,

identifying the wireless network as a wireless provisioning services supporting network, if the wireless network supports wireless provisioning services.

16. (Previously Presented) The method of claim 15, further comprising at least one of the following acts:

determining whether the wireless network is encryption enabled;

determining whether the wireless network is a Wi-Fi Protected Access (WAP) network; and,

determining whether the wireless network is a Wi-Fi Protected Access (WAP) pre-shared key network;

17. (Original) The method of claim 16, further comprising at least one of the following acts:

identifying the wireless network as unencrypted, if the wireless network is not encryption enabled; and,

identifying the wireless network as a Wi-Fi Protected Access pre-shared key network.

18. (Cancelled)

19. (Previously Presented) A data packet transmitted between two or more computer components that facilitates wireless network detection, the data packet comprising:

a data field comprising information identifying a type of available wireless network connection, the type of available wireless network detection being based, at least in part, upon iterative probing of the available wireless network, wherein automatic identification of the encryption type is based at least in part upon failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence.

20. (Cancelled)

21. (Previously Presented) A computer readable medium storing computer executable components of a wireless network detection system comprising:

a connection component that can connect a device to a plurality of wireless networks; and,

a detection component that automatically identifies a type of an available wireless network wherein identification of the encryption type is based at least in part upon failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence.

22. (Previously Presented) A wireless network detection system comprising:

means for connecting a device to a plurality of wireless networks; and,

means for automatically identifying an encryption type of an available wireless network, wherein identification of the encryption type is based at least in part upon failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence.